Strategy Research Project

PARTNERING WITH PRIVATE NETWORKS: THE DOD NEEDS A RESERVE CYBER CORPS

BY

MR. DENNIS P. DIAS
Defense Leadership & Management Program

USAWC CLASS OF 2008

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **15 MAR 2008**	2. REPORT TYPE **Strategy Research Project**	3. DATES COVERED **00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE **Partnering With Private Networks The DOD Needs a Reserve Cyber Corps**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Dennis Dias**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **Same as Report (SAR)**	18. NUMBER OF PAGES **30**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

PARTNERING WITH PRIVATE NETWORKS:
THE DOD NEEDS A RESERVE CYBER CORPS

by

Mr. Dennis P. Dias
Defense Leadership & Management Program

Mr. William Waddell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Mr. Dennis P. Dias

TITLE: Partnering With Private Networks: The DOD Needs a Reserve Cyber Corps

FORMAT: Strategy Research Project

DATE: 19 March 2008 WORD COUNT: 6,743 PAGES: 26

KEY TERMS: Networking, Cyberspace, Department of Defense, Private Sector, Inter-Agency

CLASSIFICATION: Unclassified

With the increasing rate of change of Information Technology (IT), the Department of Defense (DoD) and other government entities must look in new areas to meet threats and remain competent in this age. The concept of reaching non-uniformed civilian professionals to assist DoD in inter-agency challenges such as reconstruction in failed states can be used to suggest the use of a similar outreach to meet technology challenges. The specific challenges facing the DoD in the future will include network attacks from skilled adversaries. Given the rapid changes occurring in technology, there must be new partnerships and networks with agencies outside the DoD which should include the creation of a cyber “corps” of skilled civilian professionals that can augment DoD resources in a crisis. It is in our nation's national interest to leverage the talents of all entities in our society and the development of human intellectual capital through is critical. This Strategic Research Project (SRP) will seek to expand the concept of networking between the DoD and the private sector to create a reserve cyber “corps” to meet new technological changes and potential threats.

PARTNERING WITH PRIVATE NETWORKS

Interagency operations are becoming more common as the Department of Defense (DoD) and other government agencies seek to leverage the resources of each other to synergistically work to resolve problems of operational and strategic interest to the United States. Examples of these operations are seen in reconstruction operations conducted by civilian teams in places like Iraq and Afghanistan. As these interagency processes are strengthened, codified, exercised, and become part of the true leverage of the government elements of national power, these governmental agencies will need to look beyond the realm of the federal, state and even local governments to solve emerging new threats and problems. True leverage of national power in a democracy like the United States must also look to the private sector to leverage the immense strength that private companies offer the DoD, especially in technology related challenges. This Strategic Research Project (SRP) will seek to expand the concept of networking between the DoD and the private sector to create a cyber “corps” to meet new technological changes and potential threats. For the purposes of this paper, the focus will be on the network professionals that support DoD in both offensive and defensive IT-related operations; however the suggestions included here could map to other technology challenges.

The DoD is often the first responder to crisis’ that threaten the US. In international affairs, the Combatant Commander (COCOM) has at their disposal a great deal of national power through the military forces present to help shape regions and respond to threats. DoD responds internally to crisis’ such as natural disasters as seen in the aftermath of Hurricane Katrina, to lending expertise to domestic agencies in efforts such as training for and responding to chemical or biological attacks. DoD is well resourced, trained, and ultimately has a culture the responds and adapts to problems. The DoD has been in a cultural change – a transformation – on a continuous cycle for a very long time – although the vocabulary and pace of this change has varied at different times in our nation's history. As technology has changed at an explosive rate – thus the coining of the phrase "Moore's Law" – DoD has sought to leverage resources to adapt to the new technology. At the same time, the US experience in Iraq has demonstrated to DoD that inter-agency support is needed in many aspects of our international policy. This has created the need to integrate all departments of the government to leverage strengths in order to solve issues that arise in domestic and international affairs. However, to truly leverage the elements of national power, DoD may need to extend this network of inter-agency cooperation to the private sector to quickly tap into the resources needed to meet the fast paced challenges that new technologies present. While the DoD is well known for kinetic power and military strength – as well as non-conventional forces to meet threats – the emergence and power of smaller entities using these potentially harmful new technologies cannot be discounted. Indeed the private sector – companies, academic institutions – is routinely subjected to technology threats such as virus' and identity theft issues. While these acts may be committed by individuals or even organized crime entities, they offer a roadmap for groups with a more political purpose. Just as terrorism is the tactic chosen by groups that lack the conventional military means to challenge the US or other nation, these technological perils can be organized and directed in a manner to do harm to our nation.

While there are some specific National Strategy references that discuss specific strategies (such as the National Strategy to secure Cyberspace), many reference documents discuss the role of integrating such “cyber corps” operations into strategy and planning. The current generation of DoD policy and doctrine references are as varied as the individual service cultures. Joint policy publications tend to reference the integration of Information Operations into planning. There are references to such a program in several national level strategy documents. For example, The National Security Strategy of the United States, published in March 2006, stated:

> Developing a civilian reserve corps, analogous to the military reserves. The civilian reserve corps would utilize, in a flexible and timely manner, the human resources of the American people for skills and capacities needed for international disaster relief and post-conflict reconstruction.[1]

This policy could lay the foundation to develop the need for such a corps of professionals from the private sector that have the required IT skills to support DoD in a variety of roles. Given the wide diversity of skills in industry, these individuals could augment DoD uniformed, civilian, or even contractor personnel in facing future challenges.

Senator Lugar and Secretary Rice co-authored an op-ed article in the Washington Post that highlighted the need for funding such an idea in the creation of a “Reconstruction Reserve”[2]. This idea would create a proposed Civilian Reserve Corps, a volunteer cadre of civilian experts who would work with our military to perform the urgent jobs of post-conflict stabilization and reconstruction.[3] This example can serve as a model for similar type of program for DoD drawn from industry to counter technology challenges that could emerge quickly – inside of the cycle time to mobilize and resource traditional responses using skilled military reservists or contractors. The lessons learned from the establishment of such a construction corps could be leveraged for the “cyber corps. There are a variety of challenges – tracking skills, location of personnel, medical, security clearance statuses – all important data that DoD would need to tap to face a problem – that need to be addressed.

The federal government does have a program known as the “federal cyber service”; this program is essentially a scholarship program that targets college students majoring in key IT majors.[4] An analogy to this program could be drawn to the military Reserve Officer’s Training Corps (ROTC); just as graduates from an ROTC program go on to serve their nation in return for the tuition paid by the DoD as military officers, the graduates from the federal cyber service program serve in a variety of government-wide departments and agencies. This is an excellent start to getting IT professionals on the team of the DoD, but the pool of talent is larger than this relatively small program. However, these individuals will still work within the constraints of the DoD culture and potentially limited training opportunities. The private sector industry professionals will still have an edge as they are often working in the field that is defining and changing the very technologies the DoD seeks to leverage.

The DoD has long looked to the diversity of the private sector for new ideas; outsourcing key operations that cannot be completed efficiently within the federal government has become extremely common. However, the increasing pace of change in technology may force the government to consider the private sector in new and unique ways to maintain parity or perhaps stay ahead of the changes. This is recognized in documents designed to help the DoD begin to define and understand terms through offices such as the Office of the Assistant Secretary of Defense for

Networks and Information Integration (OASD (NII)) - which includes the DoD Chief Information Officer (CIO) and the Command and Control Research Program (CCRP).[5] The CCRP suggests that “changes are driven by changes in the environments in which the private sector operates and these developments in the private sector are a harbinger of change that provide us with an opportunity to anticipate what factors have the potential to profoundly affect military organizations and operations”. [6] Recognition of the power of the private sector by senior leaders is a first step to beginning the process of embracing the private enterprise as part of the over DoD efforts to meet technological changes. However, that leads to confusion about the domain that DoD faces these changes in.

The domain that this cooperation is, must, and will take place in is known as cyberspace. The National Strategy to Secure Cyberspace defines cyberspace as the domain “composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructure to work.” [7] This definition was probably obsolete and inaccurate before it was even published; for example, it fails to mention the millions of personal communication devices such as cellular phones that are part of the many wireless networks that operate around the globe. This point is not an attempt to define the term cyberspace, but to point out the enormous complexity of this domain. The domain does have physical locations – routers, switches, cell phone towers all have physical geographic locations, but the enormous number of applications and tools combined with the humans that use them create this complexity. At present, the public strategies published at many levels of government seem to be defensive in nature and focused on keeping networks secure.

Most National Strategy Documents and Joint Publications mention this new domain as a potential avenue of threats to the United States, but merely briefly touch on the idea of private sector integration. These strategies are just now coming to embrace interagency cooperation; this is a DoD cultural change that will take time to refine and allow leaders to develop the personal and agency-specific relationships to make it successful. It would be a huge leap for DoD to refine the interaction with the private sector when interagency operations and strategies are still being refined. Networks are already developed between the government and private sector enterprises; these are already complex inter-dependent relationships.[8] Recent scholars suggest that this may not just be about the technology; it is fundamental way government agencies need to operate in these networks; in order to "*engage complex networks of public and private actors, and the resulting need for a different style of public management, and a different type of public sector, emphasizing collaboration and enablement rather than hierarchy and control*".[9]

While the concept of interagency cooperation is embraced; and relationships are established, potential adversaries are also seeking to leverage this same technology for their own purposes. Current and future adversaries will use all technology solutions available to do damage to the United States. This damage is often thought of in terms of kinetic attacks that result in military conflict; however the attacks of 9/11 showed how a group of small well trained and financed zealots can wreak havoc on the nation physically – and more importantly, mentally. Given the unmatched power of the United States in the basic domains of warfare – air, land, and sea – adversaries will look to technology solutions to do the damage. The domains of networks under the definition of cyberspace have a variety of nations and entities seeking control. Common technology protocols established by the United States and many technology-savvy countries have created enormous advantages that allow further development and interoperatability. The very notion that these technologies are English language based is a huge strategic advantage. Thus adversaries must look for other means to seek leverage in a networked world. High technology options such as computer viruses or network disruptions can prove costly, deadly, and far reaching. Terrorist organizations use websites to post propaganda, communicate, plan, and execute operations against foes. Events in nations from Estonia to Malaysia have highlighted the prowess of adversaries in their use of network skills to damage a nation from anywhere in the world.[10] The US and other advanced nations rely heavily on secure and unsecured networks not just for the critical workings of the government, but commerce, health care, and virtually every facet of the economy. Offensive and defensive information assurance resources to protect these networks require highly trained personnel with the best tools available backed by a strategic vision that can look beyond fads and major incidents to shape the environment in a manner that allows the nation to survive and prosper. This effort requires all elements of national power – from the government to the private sector to cooperate in a manner that overcomes cultures, adversaries' decision loops, and the pace of technology itself. A reserve cyber corps of patriotic industry professionals could provide the edge in any type of conflict involving new technologies.

One key to begin the engagement with private enterprises and integrating new technology into a nation's strategy is education and training. Given the rapid changes occurring in technology, there must be new partnerships and networks with agencies outside DoD which should include commercial enterprises. Just as national strategies are embracing network centric warfare, there must be an effort to expand and formalize the training network that supports this strategy. Potential resources include other government agencies and private entities. It is critical to our nation's national interest to leverage the talents of all entities in society, and development of human intellectual capital through partnerships. However, DoD tends to look at learning in a mass-produced, repeatable, industrial age way that lends itself to large organizations. This leaves it vulnerable to an emerging threat that may rise inside of a requirements or POM cycle. Training for IT professionals in the future may not be as easy to define and track as it is being done now in the information age. The cycle time of the threat may be too short or severe – and again, only a private sector enterprise may have the professionals to deal with such a threat.

Before looking outside the government, there is interagency cooperation that is often discussed in current journals. This cooperation seeks to leverage the immense resources of the federal government across many different departments and agencies and focus them on specific objectives. It can be argued that this has always been done, but now it is receiving the attention and examination in a much more formal and institutionalized manner. The more current example of this in action is DoD working with other government agencies, from the Department of State (DOS) to the Department of Agriculture (DOA) in countries such as Iraq and Afghanistan to seek to do the complex work of rebuilding these nations into functional members of the world community. The commander of NORTHCOM has stated before Congress: "*Interagency operations are the next frontier of jointness and one that the United States should continue to foster*"[11]

This interagency approach does hint at the power of the private sector. He goes on to state how:

> In this complex interagency environment, we must also identify and transition meaningful technology that will strengthen homeland security efforts. Deliberative engagement is required across all levels of government and the private sector to support technology which enhances homeland defense and security capabilities [12]

Enterprise leadership at all levels is needed to be successful. A “top down” or “bottom up” approach may be too slow to meet a technological threat. The suggestion from a Combatant Commander also raises the question about structure. The private sector is a market-driven, chaotic group of public and private enterprises in relationships that can be allies, rivals, or neutral. There are many legal and cultural issues DoD would need to overcome to create a structure that could respond to new threats and interface in that chaos. However, the increasing pace of technological change may make this unavoidable. It may also mean that the person a CoComm looks to for a solution may look very different from the military or civilian professional they have dealt with in the past.

Leveraging the power of the private sector is not a new idea. When examining US Defense strategies for any future conflict, there is emphasis on China’s re-emergence as a world military power and potential adversary. While clearly not a positive example, the fact that China as a nation leverages national businesses for national defense could well become a key asset for that nation in the future. It can be argued that this is merely because China is a communist nation. However, to compete in the world, China has developed and removed constraints on the nation’s economy and allowed companies to operate with some degree of autonomy. However, these companies remain under some government oversight and thus are able to leverage the dual use of civilian technology to military challenges. China’s military is undergoing a self described “revolution in military affairs” that is focusing on “informationization” and clearly is embracing technology as a way to overcome the US dominance in traditional warfare.[13] In China, like any large, complicated nation there is some inherent bureaucracy that prevents this from being a smooth process, but the fact remains that China can and will use the private sector as an instrument of national power. It can then be argued that China is in fact using a sort of “cyber corps” of professionals from many levels of their society to seek a strategic advantage in warfare.

While ideally the IT needs of the DoD or Federal Government are met through cooperation, there is precedent for the government to take more emergency steps if needed. For example, the Civil Reserve Air Fleet (CRAF) and Voluntary Intermodal Sealift Agreement (VISA) are voluntary programs that help ensure access to commercial airlift and sealift in critical situations for DoD. A similar program could be established for IT threats and needs, but instead of ships and aircraft the need may be for IT services and hardware. Government takeover of IT assets, aside from clear legal issues, could easily overwhelm an agency or department, and can be argued that the collective sum of the nation’s networks are already accessible and support the nation as they are interconnected and networked as part of the “world wide web”. More than likely what would be needed is IT talent from individuals or companies that could be directed to an immediate and dynamic threat. However, to be effective, these types of programs would need to be exercised and continuously trained, and probably face a great deal of scrutiny from the private sector, congress, and the public.

To leverage the power of the commercial sector in a timely manner, there are current examples that the DoD could emulate and expand. The use of market ideas to solve government problems is not new. In 1999 the Central Intelligence Agency (CIA) created an “open” investment company called “In-Q-Tel” to obtain cutting edge technology from small, young firms traditionally reluctant to work with the federal bureaucracy; since then it has supported more than 50 companies, typically spending up to $3 million per project.[14] Funded with an approximately $35M/year, In-Q-Tel also seeks to leverage new ideas coming from academic institutions as well as commercial products like data-mining software to nanotechnology devices. [15] By functioning like a venture capital company, In-Q-Tel allows the true transfer of intellectual capital to occur without the overhead of maintaining the laboratories and personnel needed. The approach to finding private sector companies with new ideas is focused on two basic questions:

1) Is this new capability worth the funding it will require?

2) Can the Intelligence Community (IC) and, indeed, the country afford not to have this new technology? [16]

The real benefit of In-Q-Tel is the ability to reach out to companies that may lack the experience or ability to compete for federal contracts. The CIA stated that in the past much of the Agency’s technology success was the result of identifying gaps and opportunities.[17] In the age of increasing change, the strategic leader may need to focus on the gaps and opportunities; and balance the risks of these new technologies with the resources available. Resources for new technology may be difficult to find, and innovative methods like In-Q-Tel could help DoD meet new threats.

There are several such venture capital programs in the DoD; among them is the Navy’s Commercial Technology Transition Office (CTTO). The CTTO was originally created early in 1999 by the Assistant Secretary of the Navy (Research, Development, and Acquisition) and was merged with the Office of Naval Research in 2001. [18] The office has responsibilities that include promoting the rapid insertion of technology from any source by matching program needs and business strategy with technology opportunities, providing objective, independent, system-oriented technology assessments, advising on matching the Navy's business and technology insertion strategies, evaluating potentially disruptive technologies and alerting leadership to their prospects.[19] Since its inception, the CTTO has funded over 55 technology transition deals spanning a wide variety of applications, from warheads to navigation to fiber optic networking; some projects have improved warfighting capabilities, and others reduced total ownership costs.[20] The programs are more research based rather than the rapid employment of private sector resources. However, they provide access to key industry personnel to develop the personal relationships that may be needed to respond to a future crisis.

The CTTO is not without some criticism; a report from Congress pointed out that the Navy’s research and acquisition community historically has had great difficulty in transitioning innovative technologies from government research organizations and the commercial marketplace to active development and procurement programs due to the constraints of internal planning and budgeting processes, and the stifling legacy of ‘‘programs of record’’. [21] Thus, if DoD is to emulate programs like the CTTO and In-Q-Tel for more rapid fielding of solutions, there needs to be some changes made to the business processes behind the programs to ensure efficient and rapid delivery of the needed product. This also reflects the complexity of integrating such programs into the DoD portfolio, processes, and structures already in place. In addition to examining the business processes that would support cooperation with the private sector, there are additional benefits to seeking commercial technology solutions from the private sector. The market in technology, with the pace of change, often demands new products or solutions are constructed using open source standards, which will allow adaptation to new and old solutions. This can be counter to previous DoD solutions which could have been customized for a specific requirement and technologically isolated from other solutions. Further integration for technology solutions can help DoD seek to become more efficient by embracing these commercial practices, often found in software design. The cyber reserve corps personnel could help outside of technology problems – their insight could be valuable in procurement or business practices.

In some areas, both the government and private industry already have some common plans and strategies in place and already have strong partnerships. For example, disaster and recovery plans for IT networks and data are common now in large enterprises. The events of 9/11 proved what was learned on a smaller scale by firms that had lost data to natural disasters, fire, and other threats. Disaster and recovery plans varied from backup and offsite storage of data to installing duplicate networks and systems to ensure that loss or damage at a single site does not imperil the entire network. The next step – Continuity of Operations Planning (COOP) is a complete top to bottom plan for an organization to survive and operate in the event of a major disaster. The DoD had created such plans in the Cold War to ensure the continuity of elements of the Federal Government in the event of a Soviet nuclear attack. The DoD was able to leverage visioning such a scenario, the planning, resourcing, and testing of plans like this to ensure survival. Training and COOP are common grounds for DoD and industry to complement each other. With the thousands of organizations in the US developing COOP plans, there can emerge standards and best practices that can help ensure the plans are carried out in an organized and systematic approach. In turn, the multitude of options used by private companies can act as a laboratory for new ideas and concepts. The market then allows these new ideas to flourish or perish, and allow the DoD the opportunity to select ideas that have been tested. A cyber reserve corps could be part of a COOP solution.

The lateral transfer of people with these great skills into government is another alternative. Too often people outside of DoD may have selected a career opportunity and feel that serving their nation is no longer an option. The military has (as we should expect) very high standards for entry and continued employment as a military professional. By allowing people to enter and leave government there can be personnel with private sector experience that could benefit the DoD during their government time. This career opportunity can be appealing to young technology professionals given their portable retirement plans and the general understanding that one may have several careers in a lifetime. This generation offers an opportunity to shape the culture of the DoD in the coming years in a more open minded and flexible way.

The people that will lead in the coming years are now in college and have grown up with the networked technologies. No discussion of a cyber reserve corps would be completed without examining the demographics that would staff such a group. The majority of college students are now part of a new generation born in or after 1982 and most often labeled "Generation Y" but also sometimes referred to as the Net Generation, the Digital Generation, the Echo Boom Generation, or the Millennials.[22] This generation is further analyzed in Neil Howe and William Strauss' 2000 book, *Millennials Rising: the Next Great Generation*, where they described the “new generation is unique because they are more ambitious and optimistic than Generation X, are the most ethnically diverse (35 percent are nonwhite), and favor different values and learning styles than their predecessors.” [23] They are the largest child generation in American history, currently making up 34 percent of the country's population, and they are the most technologically savvy.[24] This is the generation that will lead the DoD in the future and the most likely target audience for a civilian reserve cyber corps.

Given the complexities of establishing a reserve cyber corps, a more basic idea or alternative to gain the knowledge of industry would be to allow technology sabbaticals in the private sector. This would allow DoD employees – military or civilians – to be “embedded” or work inside a successful technology organization outside of DoD to gain firsthand knowledge and build relationships with people outside of DoD. There are some ethical requirements for these select people to operate within established principals – especially related to intellectual property and proprietary requirements of a non-DoD organization, but these are not unlike current security clearance and other government requirements already in place. While these sabbaticals may be small in overall number, the personnel involved must still succeed to levels in the DoD where they could influence policy and get the resources needed to implement their ideas; not an easy task in the bureaucracy of the DoD.

Once personnel gain experience and knowledge in the areas of technology that could be of strategic benefit, how can these skills be tracked, located, and ultimately applied to a national crisis? How could such a reserve cyber corps be tapped to solve problems? How could training or exercises be conducted? There are examples of program that have sought to database skills and knowledge to leverage in times of crisis. An example can be found in the State of Pennsylvania "SERVPA" program. The State of Pennsylvania uses this program to tap into the skills and resources of the private sector. The SERVEPA website is a secure, confidential volunteer registry site that allows the State Emergency Management Agency to register, organize, and track citizens with special skills who are open to the idea of volunteering in case of an emergency.[25] This database then allows the State to leverage skills in different regions by skill sets to meet threats and challenges. There is also an "ESAR-VHP" in the Emergency System for the Advanced Registration of Volunteer Health Professionals, which can target specific skills for a large medical emergency. While the skills registered in these state programs are disaster related, this could provide a template for an IT based database of professionals to support immediate responses to technology based threats. It could be expanded to include a database of skills and companies with resources in that area as well. This, like any government issue, would take funding, oversight, and resources to maintain and protect. These are leadership challenges that can be met with present tools and laws. These examples could be emulated for a creating and maintaining a reserve civilian cyber corps.

Another benefit of having a reserve cyber corps is that it greatly expands the network of "sensors" available to DoD for new technologies and issues. Again, there are other examples in local government cooperation with industry to meet the threat – but at a smaller level. The New York City Police Department (NYPD) is well known for a number of counter-terrorism efforts, has embarked on a program known as SHIELD. SHIELD is an umbrella program for a series of current and future police department initiatives that pertain to private sector security and counter-terrorism.[26] The goal is to share information and the NYPD works with private sector personnel to “extend the network” of NYPD resources. By sharing information on suspected terrorism behaviors between the department and the private sector, the NYPD has leveraged many more “sensors” and resources to tackle such an enormous threat. Private sector contacts are organized by both industry and their geographic location in New York City. The NYPD recognized that the private sector has unique qualifications to assist the department in their pre-event planning and surveillance; in turn individuals in the private sector can be informed, participating members of the system that serves to protect their city. This partnership could serve as a model for a federal program.

No analysis of DoD-private sector interaction would be complete without examining the current construct of contracting. The question can be raised that in lieu of the resources needed to stand-up a civilian reserve cyber corps DoD could simply find a contractor to fill the requirements. The argument can be made that the DoD can leverage the national power of the private industry through contracting. Contracting or outsourcing has become a way to fill requirements in the DoD that cannot be filled with resources currently onboard. This is a very common way to leverage the power of industry – albeit at a cost – although the contracting process is expensive, not timely, and can be limited by the scope of the contracted work. Scope or mission creep that does not account for the dynamic changes in technology can impact the role of the contractor and the impact on the DoD. Contracting is a slow, deliberate process that seeks to clearly state the requirements for the contractor and allow for legal coverage to prevent fraud, waste, or abuse of government resources. Defining these requirements can be a time consuming process, and can be complicated by the changing threat of an adversary's technology. The statement of work (SOW) which delineates the work a contactor will do for the government has to be broad enough to meet challenges, yet be narrow enough to focus on a specific mission objective. The very nature of IT threats that can change dynamically can be well inside of the contracting timeline or loop. However, not all companies choose to bid for government work. Many focus exclusively on private sector enterprises or lack the resources to navigate the government contracting process. There are many companies that choose to work with the federal government and do so successfully on technology projects. Contracting has been successfully applied to large projects – even the outsourcing of entire DoD networks.

Outsourcing has been adopted for large sweeping projects before in the Department of Defense. The Navy Marine Corps Intranet (NMCI) program is an example of a large IT program that the DoD outsourced to the private sector. The NMCI was conceived as a technology solution to the emerging problem of managing many different Navy Information Technology (IT) networks that were linked together but managed independently. Navy leaders determined that the skills required to operate a completely integrated yet centrally managed IT network was outside of the Navy's "core competency" and this service could be outsourced. Outsourcing would allow the Navy to better control costs of IT and benefit from commercial best practices. Navy Leaders, in their use of environmental scanning, visioning a future requiring such a network, and leading the change within a unique military culture, succeeded in creating such a network that is managed by Electronic Data Systems (EDS), Inc.

The NMCI is actually nested under several Navy IT initiatives that are elements of defense transformation; at the top is the concept of Network-Centric Warfare (NCW)[27]. NCW focuses on using information technology tools to link aspects of military operations to leverage the strength of all assets and is believed to improve combat capability and efficiency.[28] Under this concept is a Navy program known as IT-21 – which is the Navy's investment strategy for procuring desktop workstations, networks, and related tools to establish an intranet between naval units worldwide. [29] NMCI is a part of IT-21. The outsourcing contract for NMCI was awarded to EDS in October 2000 for a cost of $6.9B for the initial five year installation, support, and periodic upgrade to the new computer network.[30] The objective of the NMCI contract was to provide over 300,000 "seats" or computer workstations that would link together on a common network and also transition some applications that users may have employed on the previous network at their work center. [31] NMCI is a program that would "touch" individual members of the Navy in a very personal way – it would impact the workstation that they would use daily for this respective mission. This makes it unique in many large DoD programs – not everyone may serve in a unit that has the latest aircraft or equipment – but all Navy personnel (uniformed and civilians) were impacted in the transition to the NMCI.

In looking outside the Navy for ideas, leaders only needed to witness the enormous IT changes that were going on in the marketplace as a result of the internet becoming widely available in the 1990s. Ironically it can be argued that this change can be traced back to the ARPANET that the DoD created as a means of connecting academic institutions supporting Research and Development efforts in the early 1970s. The marketplace took the concept and applied it to their own problems and solutions, creating the transition of the economy from manufacturing to information and services. Business organizations, in striving to be competitive, face decisions about what core products or services to maintain with finite resources. By using a strategy of focusing on key (or "core") competencies an organization could focus on what could be done best internally. Any required product or service could then be purchased from another provider. This technique is known as "outsourcing" and is done on many levels in many diverse industries. Navy leadership used this concept in deciding to pursue an outside contractor to consolidate and ultimately manage the many diverse networks and computer systems. In scanning the "IT" environment internally within the Navy and externally in search of good business practices, the Navy faced a decision. IT equipment and the related "refresh" of equipment (due to updates in software and hardware) are expensive. With the diverse number of networks maintained before NMCI, there was no integration, no process to capture and replicate best practices from other IT organizations, and uneven refresh rates for equipment. Unresolved, this would result in a large global IT enterprise that would not be well connected or best serve the dynamic mission of the Navy. The lessons learned from these experiences are often found in the IT professionals in the private sector; a cyber corps would allow those lessons to be available to DoD.

As relationships are established between DoD and private enterprises with the goal of engaging private sector intellectual capital to meet DoD threats, there is the need to exercise and test. As the old military adage "train the way you fight" is applied in the domain of cyberspace, it will help strengthen the understanding between the DoD and the private sector. In February 2006, this concept was tested in a Homeland Security exercise known as "Cyber Storm".[32] The exercise was designed to test communications, policies and procedures in response to various cyber attacks and to identify where further planning and process improvements are needed.[33] Participants in the exercise included federal and state agencies, as well as private sector "partners" from the IT, telecommunications, energy, and transportation industries, plus several foreign governments.[34] The exercise simulated a sophisticated cyber attack through a series of scenarios directed at several critical infrastructure sectors with the intent of demonstrating the interconnectedness of cyber systems with physical infrastructure and the coordination needed between public and private sectors to confront the threat.[35] These types of exercises can begin the dialog and lessons learned needed to make such relationships more functional when a real world threat emerges.

There are examples of private enterprises operating within the decision cycles of adversaries and aiding government agencies. SITE (Search for International Terrorist Entities) Intelligence Group, a small, private intelligence company was credited with acquiring a new propaganda video featuring Osama Bin Laden in September 2007 before it would have been "officially" released by al-Qaeda.[36] This firm, founded in 2002 by an Iraqi-born Israeli citizen whose father was executed by Saddam Hussein, passionately works to obtain such products through a variety of unique technology skills and tradecraft. The firm provided the video and translation to Senior US leaders, including the intelligence community. The interesting dynamic of such an organization is the blend of passion for the mission and the strength of the high technology skills. While it is impossible to learn if such techniques used to obtain the video are present within the government, the fact that a private firm was able to do this is remarkable.

While much of the above discussion has focused on cyber-defense related strategies, there are private firms that can teach offensive cyber attack skills to the DoD. One such private firm that offers training and solutions to emerging network threats is White Wolf Security of Lancaster, PA.[37] White Wolf's founder, Tim Rosenberg has developed tools and techniques to meet the threat for government and private industry in what he terms "the cross domain" elements of warfare.[38] Rosenberg believes that the DoD warrior of the future will need these technology skills along with the traditional military skills that have been taught for generations. Unlike many security firms, White Wolf also offers training and white papers on offensive operations, all which are in the unclassified domain. Again, the unique blend of passion, understanding the domain and the threats, backed up by cutting edge technology skills can provide the training and expertise to meet the threat.

The Department of Defense faces unique threats in the domain of cyberspace. This new domain offers adversaries a venue to attack the US in unconventional ways that can do serious physical and economic damage. To meet this threat, the DoD must seek new partnerships with the private sector, who often are the leaders in technology solutions. The decision loop for responding to threats in this domain may be well inside of traditional DoD responses and may even begin in the private sector networks. While with any transformation of the DoD – time and resources are needed. However, the war in this domain may have already begun. As GEN (R) Barry Mccaffrey recently wrote as part of his assessment of the US Air Force:

> We must expand exponentially the resources, R&D, and human talent devoted to the massive and on-going war against our US communications-computer-control systems. This is the "poor man's" Weapon of Mass Destruction. Every classified brief I receive underscores the absolute certainty that all our potential adversaries, terrorist organizations, and many private criminal groups conduct daily electronic reconnaissance and probes of the electro-magnetic spectrum and devices which are fundamental to our national security strategy. We lead the world in technical creativity in these associated engineering and scientific areas… We must sort out clearly the international legal and policy considerations upon which we will base widely understood Joint Directives governing the centralized employment of offensive cyber-warfare. This is the first sword to unsheathe in time of modern combat. [39]

The establishment of civilian reserve cyber corps to augment the U.S. DoD which is facing enormous and evolving challenges in the future is a recommendation that bears merit and has a variety of supporting programs that could be leveraged. Such a corps of professionals helps leverage all aspects of national power in a complex world that brings new technologies that have the potential to do great harm to our nation.

Endnotes

[1] George W. Bush, *The National Security Strategy of the United States of America;* (Washington, DC: The White House, March 2006), 45.

[2] Richard G. Lugar and Condoleezza Rice, "A Civilian Partner for Our Troops; Why the U.S. Needs A Reconstruction Reserve," *The Washington Post*, 17 December 2007, available from http://www.proquest.com/; Internet; accessed 20 December 2007.

[3] Ibid.

[4] "Federal Cyber Service: Scholarship for Service," available from https://www.sfs.opm.gov; Internet; accessed 23 February 2008.

[5] *Department of Defense Chief Information Officer Home Page*, available from http://www.defenselink.mil/cio-nii/; Internet; accessed 11 November 2007.

[6] Alberts, David S., John J. Garseka, and Frederick P. Stein. *Network Centric Warfare Developing and Leveraging Information Superiority (*Washington D.C.: DoD C4ISR Cooperative Research Program, 2001) available from http://www.dodccrp.org/files/Alberts_NCW.pdf; Internet; accessed 28 October 2007.

[7] *The National Strategy to Secure Cyberspace*, February 2003. available from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf; Internet; accessed 18 October 2007.

[8] It can be argued that the various agencies networks, connected via the "internet" are in fact already networked but in the basic form.

[9] Lisa Blomgren Bingham, Tina Nabatchi, and Rosemary O'Leary, "The New Governance: Practices and Processes for Stakeholder and Citizen Participation in the Work of Government," *Public Administration Review* 65 (1 September 2005): 547, available from http://www.proquest.com/; Internet; accessed 2 January 2008.

[10] Jim Melnick, "The Cyberwar against the United States," *The Boston Globe*, 19 August 2007, newspaper on-line, available from http://www.boston.com/news/globe/editorial_ opinion/oped/articles/2007/08/19/the_cyberwar_against_the_united_states/; Internet; accessed 20 August 2007.

[11] U.S. Congress, House Armed Services Committee, Testimony by ADM Timothy Keating, Statement to the House Armed Services Committee, 21 March 2007, available from http://www.house.gov/hasc/hearing_information.shtml; Internet; accessed 03 October 2007.

[12] Ibid.

[13] Dr. Michael A. Weinstein, "China Punches Below Its Weight – For Now," *Asia Times*, 08 January 2005, newspaper on-line, available from http://www.atimes.com/atimes/China/ GA08Ad01.html; Internet; accessed 09 November 2007.

[14] David Malakoff "CIA Looks to Universities for Cutting-Edge Tools, "*Science* 304, no. 5667 (2 April 2004): 30, available from http://www.proquest.com/; Internet; accessed 4 January 2008).

[15] Ibid.

[16] *In-Q-Tel Home Page*, available from http://www.inqtel.org/about/index.htm; Internet; accessed 09 October/2007.

[17] Ibid.

[18] *The Office of Naval Research Commercial Technology Transition Officer Homepage,.* available from http://www.onr.navy.mil/ctto/about.asp; Internet; accessed 19 December 2007.

[19] Ibid.

[20] Ibid.

[21] *Department Of Defense Appropriations Bill, 2003 Report Of The Committee On Appropriations [To Accompany H.R. 5010]* 107th Congress, 2nd Session., 2003, available from http://www.fas.org/asmp/resources/govern/107th_hr5010_rpt532.pdf; Internet; accessed 20 December 2007.

[22] Susan Gardner and Susanna Eng, "What Students Want: Generation Y and the Changing Function of the Academic Library," *Portal : Libraries and the Academy* 5, no. 3 (1 July 2005): 405-420, available from http://www.proquest.com/; Internet; accessed 09 January 2008.

[23] Ibid.

[24] Ibid.

[25] *The SERVPA Home Page*, available from https://www.servpa.state.pa.us/; Internet; accessed 15 October 2007.

[26] *The NYPD SHIELD Home Page,* available from http://www.nypdshield.org; Internet; accessed 20 November 2007.

[27] Ronald O'Rourke, "Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress," available from http://www.history.navy.mil/library/online/navy_ network.htm; Internet; accessed 03 October 2007.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Department of Homeland Security, "Fact Sheet: Cyber Storm Exercise;" Release Date September 13, 2006, available from http://www.dhs.gov/xnews/releases/pr_ 1158340980371.shtm; Internet; accessed 20 December 2007.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Joby Warrick "Leak Severed a Link to Al-Qaeda's Secrets; Firm Says Administration's Handling of Video Ruined Its Spying Efforts;" *The Washington Post*, 9 October 2007, available from http://www.proquest.com/; Internet; accessed 10 October 2007.

[37] *The White Wolf Security Company Home Page*. available from http://www.whitewolfsecurity.com/; Internet; accessed numerous times September 2007-January 2008.

[38] Rosenberg, Timothy. Founder, White Wolf Security Company, Lancaster, PA, telephone interview with the author, 04 October 2007.

[39] GEN (R) Barry R. McCaffrey, USA, “After Action Report Visit to Nellis And Scott AFB 14-17 AUGUST 2007” — dated 15 October 2007 for COL Mike Meese, US Military Academy. 16 October 2007 email from Academic Dean posted on Dean’s Corner, US Army War College.